UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/396,054	09/15/1999	YOSHIHITO ISHIBASHI	09812.0583-00000	6914

22852 7590 01/24/2007

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
ABEL JALIL, NEVEEN	
ART UNIT	**PAPER NUMBER**
2165	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/396,054	ISHIBASHI, YOSHIHITO	
	Examiner	Art Unit	
	Neveen Abel-Jalil	2165	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,14-16,18, 20-25,29-34 and 38-41* is/are rejected.

7)☒ Claim(s) *6-13,17,19,26-28 and 35-37* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on November 3, 2006, PROSECUTION IS HEREBY REOPENED. *A new ground of rejection is* set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

C Rones

2. Claims 1-41 are now pending.

3. Applicant's arguments were deemed to be persuasive therefore; the previous 35 USC 101, and 112, second rejections have been withdrawn.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,784,464 to Akiyama et al. in view of U.S. Patent No. 5,319,705 to Halter et al.

Note: U.S. Patent No. 5,784,464 to Akiyama et al. was cited in the first office action.

As to claims 1, and 20, Akiyama et al. discloses an information retrieval system and key distribution system including encrypting a random number with a first key in response to content access request, and a second authenticator by generating a second key and encrypting the first key, generating yet a third key, decrypting the keys, and logging said information (see column 3, lines 1-23).

Though Akiyama et al. does disclose a method for authenticating a client with a key stored before hand in the client, Akiyama et al. also further suggests that any known way of generating, storing, or transmitting a key may be used and also suggests that multiple keys can be generated (see column 4, lines 12-38).

The access system disclosed by Halter includes the sending of encrypted decryption keys being sent to a customer by the same means as the encrypted software being purchased, as well the sending to the customer a "customer key" for decrypting the encrypted file key. Halter also discloses the changing of the keys when a new group of files is acquired (see column 5, line 65 to column 6, line 24). Halter further suggests that this is done to prevent files from being decrypted except at appropriate user processors (see column 4, lines 48-59).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Akiyama et al. by using the key distribution

system disclosed by Halter, in order to prevent files from being decrypted except at appropriate user processors.

As to claims 2, and 21, Akiyama et al. as modified discloses further comprising the storage key generating means for generating the second storage key by means of a random number generator (See Akiyama et al. column 11, lines 59-65, also see Halter et al. abstract).

As to claim 3, Akiyama et al. as modified discloses wherein the decrypted content key is encrypted with identification information of the user equipment and stored into the user equipment (See Akiyama et al. column 7, lines 1-8, also see Halter et al. abstract).

As to claim 4, Akiyama et al. as modified discloses wherein the content key is encrypted, in the user equipment, with the first storage key and identification information of the user equipment, and the content key stored in the user equipment is decrypted with the first storage key and the identification information of the user equipment (See Akiyama et al. column 4, lines 15-25, also see Halter et al. abstract).

As to claim 5, Akiyama et al. as modified discloses wherein the second storage key is generated by a decrypted key generating means provided in the user equipment (See Akiyama et al. column 4, lines 15-25, also see Halter et al. abstract).

As to claims 14, 29, and 38, Akiyama et al. as modified discloses wherein the user equipment has stored therein identification information of the user equipment (See Akiyama et al. Figure 9, 11, 12, databases, also see Akiyama et al. column 3, lines 1-5, and column 7, lines 1-8).

As to claims 15, and 30, Akiyama et al. as modified discloses wherein the data storage starts decrypting the content key stored in the second storing means depending on the result of inspection of the identification information of the data storage, stored in the second storing means (See Akiyama et al. Figure 10, S23, wherein "result of inspection" reads on "comparator").

As to claim 16, Akiyama et al. as modified discloses as modified wherein the decrypted content key supplied from the user storing has added thereto information that the content key has been obtained by restoration (See Akiyama et al. column 7, lines 25-31).

As to claims 18, and 41, Akiyama et al. as modified discloses wherein the content key has added thereto frequency information which limits the number of times the content key can be used (See Akiyama et al. Figure 12, S34, counter value, also see Akiyama et al. column 10, lines 15-20).

As to claim 22, Akiyama et al. as modified discloses wherein the encrypting means encrypts the decrypted content key with identification information of a second storing means (See Akiyama et al. column 12, lines 10-18).

As to claim 23, Akiyama et al. as modified discloses wherein the content key is encrypted, in the first storing means, with the first storage key and identification information of the first storing means (See Akiyama et al. column 12, lines 10-18); and

the content key stored in the first storing means is decrypted with the first storage key and the identification information of the first storing means (See Akiyama et al. column 12, lines 10-18).

As to claims 24, and 31, Akiyama et al. as modified discloses wherein the first storing means, first decrypting means, and encrypting means form together a data storage, wherein the key management unit manages the second storage key of the data storage (See Akiyama et al. column 7, lines 25-35).

As to claims 25, and 32, Akiyama et al. as modified discloses wherein the data storage is a data receiver which receives a content data encrypted and sent from a data transmitter (See Akiyama et al. column 5, lines 32-43).

As to claim 33, Akiyama et al. as modified discloses wherein the key management unit comprises an identification information storing means in which the identification information of the first storing means is stored (See Akiyama et al. column 7, lines 1-8).

As to claim 34, Akiyama et al. as modified discloses wherein the key management unit accounts the data service following the predetermined procedure depending upon a generation of the second storage key (See Akiyama et al. column 3, lines 1-5).

As to claim 39, Akiyama et al. as modified discloses wherein the data storage starts decrypting the content key stored in the second content storing means (See Akiyama et al. column 3, lines 17-19).

As to claim 40, Akiyama et al. as modified discloses wherein the content key obtained by decryption from the second storing means has added thereto information that the content key has been obtained by restoration, as requirement information (See Akiyama et al. column 15, lines 1-21).

Allowable Subject Matter

6. Claims 6-13, 17, 19, 26-28 and 35-37 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

7. Applicant's arguments with respect to claims 1-41 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. For list of cited references, see PTO-Form 892.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Neveen Abel-Jalil whose telephone number is 571-272-4074. The examiner can normally be reached on 8:30AM-5:30PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey A. Gaffin can be reached on 571-272-4146. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Neveen Abel-Jalil
August 20, 2006

DETAILED ACTION

Remarks

1. In response to Amendment filed on March-13-2006, claims 1-41 are presently pending in the application.

Claim Objections

2. Claims 18, and 41 are objected to because of the following informalities:

Claims 18, and 41, line 3, both recite "can be used" which is optional recitation indicating the limitaion following never having to take place and thus the step of the claim not to carry any patentable weight. Claim should be amended to recite more direct and definite language such as "when" or "wherein" or "is". The exact recitation of "used" is intended use and does not carry any patentable weight. Claim should be amended to recite more direct and positive language.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 1 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 1 is not statutory because it merely recite a number of computing steps without producing any tangible result and/or being limited to a practical application (see MPEP 2106 IV.B.2.(b)). In claim 1, the steps of "storing...sending ... and sending" are not hardware interrelated. They are software per se and require a computer/hardware in order to

realize their functionality. The claim should be amended to recite a storage hardware or computer. Although the preamble recites "user equipment", there is not enough indication in the specification for the equipment to be defined as computer or database or processor of any sorts to perform the steps of the method.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 8, 10, 13, 18, 24-30, 34-37, and 39-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claim 8, line 6, the recitation of "following a predetermined procedure" renders the claim to be indefinite for failing to determine the scope of the claimed invention since the metes and bounds of predetermined procedure would not be understood by the skilled artisan because such standards are subject to change over time. The procedures are modifiable with time. A claim cannot be definite when it has different meanings at different times.

Independent claims 10, 13, 28, and 34 carry the same deficiency.

Claims 8, 28, and 34 recites the limitation "the data service" in line 5. There is insufficient antecedent basis for this limitation in the claim.

Claims 18, and 41 recites the limitation "the number of times" in various lines. There is insufficient antecedent basis for this limitation in the claim.

Claims 24, 25, 27, 29, and 30 recites the limitation "the data storage" in various lines. There is insufficient antecedent basis for this limitation in the claim.

Claim 26, recites the limitation "the second content storing means" in various lines. There is insufficient antecedent basis for this limitation in the claim.

Claims 27, 28, 29, 30, 35, 36, 37, 39, and 40, all recite the limitation "the second storing means" in various lines. There is insufficient antecedent basis for this limitation in the claim.

Claims 30, recites the limitation "the result of the inspection" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 40, line 4, recite "as requirement information" which is vague and confusing since the Examiner is not sure what is being referenced here. Correction is required.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

8. Claims 1-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Akiyama et al. (U.S. Patent No. 5,784,464).

As to claim 1, Akiyama et al. discloses a content management method for managing content data provided to user equipment, comprising the steps of:

storing a content key encrypted with a first storage, content data encrypted with the content key, and a second storage key in the user equipment (See Figure 9, 11, 12, databases, also see column 3, lines 1-5, and column 7, lines 1-8);

sending the encrypted content key and the second storage key to a key management unit (See Figure 8, key mgmt. Unit);

at the key management unit, decrypting the encrypted content key using the first storage key, the first storage key being stored in the key management unit (See Figure 10, S23); and

encrypting the decrypted content key using the second storage key (See column 14, lines 45-56);

sending the content key encrypted with the second storage key along with the encrypted content to the user equipment (See column 3, lines 17-19); and

at the user equipment, decrypting the content data using the decrypted content key (See column 3, lines 17-19).

As to claims 2, and 21, Akiyama et al. discloses further comprising the storage key generating means for generating the second storage key by means of a random number generator (See column 11, lines 59-65).

As to claim 3, Akiyama et al. discloses wherein the decrypted content key is encrypted with identification information of the user equipment and stored into the user equipment (See column 7, lines 1-8).

As to claim 4, Akiyama et al. discloses wherein the content key is encrypted, in the user equipment, with the first storage key and identification information of the user equipment, and the content key stored in the user equipment is decrypted with the first storage key and the identification information of the user equipment (See column 4, lines 15-25).

As to claim 5, Akiyama et al. discloses wherein the second storage key is generated by a decrypted key generating means provided in the user equipment (See column 4, lines 15-25).

As to claim 6, Akiyama et al. discloses wherein the second storage key is encrypted with a public key for the key management unit for management of the storage keys to generate a third storage key and the third storage key is stored into the user equipment (See column 3, lines 29-41).

As to claims 7, and 36, Akiyama et al. discloses wherein the user equipment deletes the second storage key depending upon whether the third storage key has been stored in the user equipment (See column 7, lines 25-31).

As to claim 8, Akiyama et al. discloses wherein when decrypting the content key stored in the second content storing means, the user equipment sends the third storage key to the key management unit; and the key management unit generates the second storage key based on the third storage key while accounting the data service following a predetermined procedure (See column 12, lines 1-9).

As to claim 9, Akiyama et al. discloses wherein the second storage key is generated by a storage key generating means provided in the key management unit which manages the storage keys; and the key management unit has stored therein the second storage key and the identification information of the user equipment in which the content key encrypted with the above generated second storage key is stored (See column 7, lines 25-31).

As to claim 10, Akiyama et al. discloses wherein upon the generation of the second storage key, the key management unit accounts the data service following the predetermined procedure (See column 10, lines 15-20).

As to claim 11, Akiyama et al. discloses wherein the key management encrypts the second storage key with the management key to generate a third storage key, and sends the third storage key to the user equipment; and the user equipment stores the received third storage key (See column 3, lines 31-41, also see column 14, lines 35-43).

As to claims 12,and 27, Akiyama et al. discloses wherein the data storage deletes the second storage key depending upon whether the third storage key is stored in the second storing means (See column 3, lines 31-41).

As to claims 13, and 37, Akiyama et al. discloses wherein the key management unit has stored therein the identification information of the user equipment storing means in which the content key encrypted with the second storage key is stored (See Figure 9, 11, 12, databases, also see column 3, lines 1-5, and column 7, lines 1-8);

the user equipment sends, when decrypting the content key stored in the user equipment, the identification information of the user equipment to the key management unit (See column 18, lines 10-17); and

the key management unit generates the second storage key based on the result of comparison between identification information of the user equipment sent from the user

equipment, and the identification information of the user equipment, held in the key management unit itself, while accounting the data service following the predetermined procedure (See column 7, lines 25-35).

As to claims 14, 29, and 38, Akiyama et al. discloses wherein the user equipment has stored therein identification information of the user equipment (See Figure 9, 11, 12, databases, also see column 3, lines 1-5, and column 7, lines 1-8).

As to claims 15, and 30, Akiyama et al. discloses wherein the data storage starts decrypting the content key stored in the second storing means depending on the result of inspection of the identification information of the data storage, stored in the second storing means (See Figure 10, S23, wherein "result of inspection" reads on "comparator").

As to claim 16, Akiyama et al. discloses wherein the decrypted content key supplied from the user storing has added thereto information that the content key has been obtained by restoration (See column 7, lines 25-31).

As to claim 17, Akiyama et al. discloses wherein when moving the content key having added thereto the information that the content key has been obtained by restoration, the user requirement performs an error process based on the result of comparison between the content key and another content key stored in a destination to which the content key is to be moved (See column 15, lines 1-21).

As to claims 18, and 41, Akiyama et al. discloses wherein the content key has added thereto frequency information which limits the number of times the content key can be used (See Figure 12, S34, counter value, also see column 10, lines 15-20).

As to claim 19, Akiyama et al. discloses further comprising storing the content key encrypted with the second storage key in a first storage of the user equipment along with identification information of the first storage; storing the content key that is stored in the first storage, and the identification information of the first storage, into a second storage of the user equipment (See Figure 9, 11, 12, databases for storage);

performing, when a request is made to decrypt the content key in the first storage, an error process based on the result of the comparison between the identification information of the first storage and the identification information of the second storage (See column 15, lines 1-21).

As to claim 20, Akiyama et al. discloses a content management system for managing content data, comprising:

a first storing means having stored therein a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key (See Figure 9, 11, 12, databases, also see column 3, lines 1-5, and column 7, lines 1-8);

a first sending means for sending the encrypted content key and the second storage key to a key management unit (See Figure 8, key mgmt. Unit);

a first decryption means, in the key management unit, for decrypting the encrypted content key using the first storage key being stored in the key management unit (See Figure 10, S23);

an encrypting means for encrypting the decrypted content key using the second storage key (See column 14, lines 45-56); and

a second decrypting means for decrypting the encrypted content using the second storage key and decrypting the content data using the decrypted content key (See column 3, lines 1-20).

As to claim 22, Akiyama et al. discloses wherein the encrypting means encrypts the decrypted content key with identification information of a second storing means (See column 12, lines 10-18).

As to claim 23, Akiyama et al. discloses wherein the content key is encrypted, in the first storing means, with the first storage key and identification information of the first storing means (See column 12, lines 10-18); and

the content key stored in the first storing means is decrypted with the first storage key and the identification information of the first storing means (See column 12, lines 10-18).

As to claims 24, and 31, Akiyama et al. discloses wherein the first storing means, first decrypting means, and encrypting means form together a data storage, wherein the key management unit manages the second storage key of the data storage (See column 7, lines 25-35).

As to claims 25, and 32, Saito discloses wherein the data storage is a data receiver which receives a content data encrypted and sent from a data transmitter (See column 5, lines 32-43).

As to claim 26, Akiyama et al. discloses comprising means for storing a public key of the key management unit; and wherein the second content storing means has stored therein the second storage key along with a third storage key obtained by encrypting the second storage key with the public key (See column 3, lines 31-41).

As to claim 28, Akiyama et al. discloses wherein when decrypting the content key stored in the second storing means, the data storage sends the third storage key to the key management unit; and the key management unit sends the second storage key generated based on the third storage key to the data transmitter while accounting the data service following a predetermined procedure (See column 12, lines 1-9).

As to claim 33, Akiyama et al. discloses wherein the key management unit comprises an identification information storing means in which the identification information of the first storing means is stored (See column 7, lines 1-8).

As to claim 34, Akiyama et al. discloses wherein the key management unit accounts the data service following the predetermined procedure depending upon a generation of the second storage key (See column 3, lines 1-5).

As to claim 35, Akiyama et al. discloses wherein the key management unit comprises means for storing storage keys;

the key management unit generates a third storage key by encrypting the second storage key with a management key and sends the third storage key to the data storage (See column 3, lines 29-41); and

the data storage stores the third storage key into the second storing means (See column 4, lines 1-21).

As to claim 39, Akiyama et al. discloses wherein the data storage starts decrypting the content key stored in the second content storing means (See column 3, lines 17-19).

As to claim 40, Akiyama et al. discloses wherein the content key obtained by decryption from the second storing means has added thereto information that the content key has been obtained by restoration, as requirement information (See column 15, lines 1-21).

Response to Arguments

9. Applicant's arguments with respect to claims 1-41 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-Form 892 for list of cited references.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Neveen Abel-Jalil whose telephone number is 571-272-4074. The examiner can normally be reached on 8:30AM-5:30PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey A. Gaffin can be reached on 571-272-4146. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Neveen Abel-Jalil
May 28, 2006